U.S. Department of Commerce
National Oceanic & Atmospheric Administration

Privacy Impact Assessment for the NOAA0900 Consolidated Cloud Applications

Reviewed by: Mark Graff Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 2/23/2022

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/OCIO/Consolidated Cloud Applications

Unique Project Identifier: NOAA0900

Introduction: System Description

NOAA0900 is a consolidated accreditation boundary for multiple existing NOAA cloud applications, as well as any new cloud applications. NOAA Consolidated Cloud Applications' component cloud applications are distributed among multiple Cloud Service Providers (CSP).

This is an aggregated system with multiple applications, which are connected through NOAA networks to various Cloud service Providers. These applications are as follows:

Everbridge Suite (EBS)

EBS is a Software-as-a-Service platform that is used for managing critical events. Federal Agencies and other organizations use EBS platform for operational response to critical events in order to keep people safe and businesses running faster. During public safety threats such as active shooter situations, terrorist attacks or severe weather conditions, as well as critical business events such as IT outages, cyber-attacks or other incidents such as product recalls or supply-chain interruptions, customers rely on the EBS platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes, and track progress on executing incident response plans. Many Federal agencies utilize EBS as part of their employee communication strategy – for agency's contingency planning and business continuity, staff augmentation, and IT Alerting needs.

Google Workspace

Google Workspace is a collection of cloud computing, productivity, and collaboration tools, software and products. It includes email, calendar, contacts, chat, drive, and meet for users.

Maas 360

MaaS360 configures mobile devices using the DoD Security Technical Implementation Guide (STIG) cybersecurity baseline. MaaS360 offers scale, control and security across all devices and mobile platforms, providing total device management by user, device, application, and across an enterprise. As a fully integrated cloud platform, MaaS360 delivers Mobile Device Management (MDM) to customers.

ServiceNow

The ServiceNow product is a suite of natively integrated applications designed to support IT service automation, resource management and shared support services. ServiceNow is built on modern web technologies. The ServiceNow platform includes easy-to-use, point-and-click customization tools to help customers create solutions for unique business requirements.

SmartSheet

SmartSheet provides a cloud collaboration platform to enable users to plan, capture, manage, automate, and report on work while utilizing various collaboration features. SmartSheet projects provide essential tools for project management.
Smartsheet collects the following information: Administrative Data; Financial Administration (IT Acquisition workflows); IT Ticket System (Help Desk); and Project/Program Management.

Ivanti

Ivanti Service Manager (ISM) is a cloud-based IT Service Management (ITSM) solution. ISM is designed to be the central point of contact between users, employees and the IT organization. It offers first and second line support to users, where incidents, problems or inaccuracies in IT systems are reported.

AODocs

AODocs is a document management system which is used distribute Standard Operating Procedures, manage quality control processes, and assist in the coordination of contract management, procurements, intranet publication and incident reporting.

Esri

Esri is an international supplier of geographic information system (GIS) software, web GIS, and geodatabase management applications. There are several custom applications, mostly web-based, that are used to input, process, and provide access to a myriad of scientific and administrative data.

Esri, a geospatial cloud which hosts ArcGIS data as web layers, allows complex datasets on easy-to-understand smart maps, which are used to visualize and monitor important trends across lines of business and take action in mission-focused projects. A geospatial cloud also allows location intelligence data to be easily combined with artificial intelligence and predictive analytics to map out ways to drive productivity or adjust strategies before bigger problems develop.

CloudCheckr

The CloudCheckr system is a cloud cost and security management tool that allows companies to review cost, inventory, security, compliance, and utilization information about their cloud environments. Customers can drill down for more information on each check, customize the CloudCheckr dashboards that are displayed, set up alerts and notifications, or create and export reports.

Avaya OneCloud

Avaya OneCloud For Government is a family of real-time and near-real-time enterprise-grade applications for Unified Communications, Contact Center/Customer Experience (CX) and voice/video/web collaboration. The solution is comprised of the following elements as part of the standard offering:

- MPLS network as transport (or optional 3rd party transport – agreed upon between Avaya and said Agency) provided by Service Provider partners
- Avaya OneCloud For Government Hosting Facilities
- Avaya OneCloud For Government Network Operations Centers (NOCs) - Avaya facilities in Columbia, MD and Coppell, TX
- SIP Trunking to the PSTN (via existing agency carrier) for inbound and outbound PSTN calling
- CPE - Installation and Maintenance Options
- Optional customized solutions to integrate into Government customer environments

Qualtrics

Qualtrics is a simple to use web-based survey tool to conduct survey research, evaluations and other data collection activities.
https://www.osec.doc.gov/opog/PrivacyAct/sorns/GOV-Wide/GSA-GOV7-2015-26940.pdf

Entellitrak

Entellitrak is an enterprise level COTS (Commercial Off-The-Shelf) that provides unified BPM software by using an open architecture approach that focuses on the core technologies that streamline work for rapid application development on business processes. Entellitrak provides all of the functionality required to collect, track, manage, process, and report on information regarding a business process.

NOAA0900 does collect and display photographs of employees and contractors on some websites in support of education and outreach. Notice and consent is provided prior to collecting, storing, and using these images.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

NOAA0900 is a General Support System.

(b) System location

NOAA OCIO offices are located at the Silver Spring Metro Center (SSMC) campus in SSMC3 at 1315 East West Highway, Silver Spring, Maryland

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

This is an aggregated system with multiple applications, which are connected through NOAA networks to various Cloud service Providers. These applications are as follows:

Application Names	**ATO status**	**FIPS-199 Categorization**
Everbridge Suite (EBS)	FedRAMP ATO	MODERATE
Google Workspace	FedRAMP ATO	MODERATE
Maas 360	FedRAMP ATO	MODERATE
ServiceNow	FedRAMP ATO	HIGH
SmartSheet	FedRAMP ATO	MODERATE
Ivanti	FedRAMP ATO	MODERATE
AODocs	NOAA Approved	MODERATE
Esri	FedRAMP ATO	LOW
CloudCheckr	FedRAMP Ready	MODERATE
Avaya One Cloud	FedRAMP ATO	MODERATE
Qualtrics	FedRAMP ATO	MODERATE
Entellitrak	FedRAMP ATO	MODERATE

(d) The way the system operates to achieve the purpose(s) identified in Section 4

As the system is an aggregate system, NOAA0900 provides overall management and security support.

(e) How information in the system is retrieved by the user

NOAA0900 applications information is accessed by authorized personnel in order to deliver a variety of support information. Users authenticate via NOAA ICAM (Identity, Credential, and Access Management Services).

(f) How information is transmitted to and from the system

NOAA0900 applications information is accessed by authorized personnel via NOAA networks and multiple CSPs in order to deliver a variety of support information. All traffic is encrypted during transit utilizing FIPS-140-2 compliant cryptographic modules.

(g) Any information sharing conducted by the system

EBS collects the following information: name, work phone number, work cell phone number, work email address, work mailing address, organization data, and account data.

Google Workspace collects email logs, authentication logs, basic user information, device information, calendar logs, and drive logs. Data Owners (customers) determine what content is stored in Google Workspace and with whom that content is shared.

MaaS360 collects basic user information and basic device information. MaaS360 does not collect PII or BII.

ServiceNow collects user information such as name, user information related to injuries, deaths, incident information, and mishaps that occur to those users, and IT Ticket information. Data Owners (customers) determine what content is stored in ServiceNow and with whom that content is shared.

Smartsheet does not collect PII or BII. Data Owners (customers) determine what content is stored in SmartSheet and with whom that content is shared.

Ivanti does not collect BII or PII.

AODocs: Commerce Alternative Personnel System (CAPS) performance evaluations, safety and protocol documents related to marine operations, marine engineering drawings and correspondence, and other generic file-sharing repositories.

Esri collects basic organizational profile information such as username, email, and a biography. Esri does not collect any PII or BII.

CloudCheckr does not collect any PII or BII.

Avaya One Cloud collects Name, Phone, Number, Email, Location, and Voicemail.

Qualtrics: Survey Owners (customers) determine what content is stored in Qualtrics and with whom that content is shared.

Entellitrak PII collected in the system consists of: employee’s or applicant’s name, functional limitation caused by the disability, reasonable accommodation (RA) requested, explanation of how RA would assist the applicant in the application process or the employee in performing his/her job or receiving the benefits and privileges of employment, dates when the required interactive discussions were held, notes from discussion regarding the request, action by deciding official, whether medical documentation was sought, justification for requesting medical documentation, any sources of technical assistance that were consulted, and if the request was denied, the reason for denial (but not medical documentation, which will be kept in a separate file).

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

5 U.S.C. chapters 11, 33, and 63
5 U.S.C. 301, 1104, 1302, 2951, 3301, 3321, 3372, 4118, 4305, 5379, 5405, and 8347
26 U.S.C. 6402(d)
28 U.S.C. 533-535, 3101-3105
31 U.S.C 66a, 492, 3711
35 U.S.C. 2
41 U.S.C. 433(d)
44 U.S.C. 3101, 3309

5 CFR Part 229, 339, 537
Executive Orders 9397, as amended by 13478, 9830, and 12107, 12196, 12564, 12656, and 13164
DAOs 202-957 and 210-110
Debt Collection Act of 1982 (Pub. L. 97-365)
Federal Preparedness Circular (FPC) 65, July 26, 1999
Public Law 100-71, dated July 11, 1987.
The Electronic Signatures in Global and National Commerce Act, Public Law 106-229; Homeland Security Presidential Directive 12
IRS Publication-1075
The National Marine Sanctuaries Act. 16 U.S.C. 1440 with the support for research monitoring and education

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

This is a FIPS 199 High system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_X___ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging	X	g. New Interagency Uses	
b. Anonymous to Non- Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes	X	f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): The following applications have been added to NOAA0900 since the last PTA was conducted: CloudCheckr Avaya OneCloud Qualtrics Entellitrak The following applications no longer fall under NOAA0900: MS Dynamics Virtru COVID vaccination information has been added to the system.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	X
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	X
e. File/Case ID	X				
n. Other identifying numbers (specify):					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

Human Resources matters including performance appraisals, bonus structures, pay issues, disciplinary actions. Each PII piece is shared with the LO that NOAA0900 is hosting their application for and any subsequent sharing is identified in their individual PIA.

Medical records are imported into the AODocs library and protected using Google Drive's FIPS-140-2 compliant encryption at rest and the Google Common Infrastructure. AODocs may contain Protected Health Information (PHI) or PII such as full name, SSN, date of birth and email address.

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name		i. Place of Birth	X	p. Medical Information	X
c. Alias		j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	
f. Race/Ethnicity		m. Education	X	t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify): Covid vaccination record as a condition of employment.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording	X	h. Eye Color		m. DNA Sample or Profile	
d. Video Recording	X	i. Height		n. Retina/Iris Scans	X
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

All applications are ensuring accuracy based on FedRAMP requirements and adheres to the compliance standards of the Federal Information Processing Standard (FIPS). FedRAMP security controls encompass the accuracy, confidentiality, integrity, and availability of the information.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. There is a PRA collection for Ernest Hollings (0648-0568) and Dr. Nancy Foster scholarship (0648-0432)
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	

Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			
	There are not any IT system supported activities which raise privacy risks/concerns.		

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	X
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	X
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	

Other (specify):
EBS communicates with NOAA staff prior to, during, and after all-hazards or emergency events.

AODocs – HR information is collected for the purpose of pay alignment, HR performance reporting, and HR management efforts. AODocs also collects BII for administering healthcare. BII that is specifically related to commercial contracts and financial information is collected for management, administration and information sharing. Only encrypted PII/PHI is stored in AODocs (Google Drive's FIPS-140-2 compliant encryption at rest) to share sensitive personal and medical data securely in compliance with the Health Insurance Portability and Accountability Act (HIPAA). Customer related metadata is stored on Google App Engine DataStore which is FedRAMP approved, but not included under the NOAA Google ATO.

Note: A majority of the SaaS applications under NOAA0900 allow the Data Owners to determine what content is stored, and with whom that content is shared.

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NOAA ENS is a cloud-based, software-as-a-service, vendor-hosted mass notification system that provides tools for reaching pre-defined contacts during an emergency situation. The purpose of the Emergency Notification System is to simplify management of emergency communication processes and procedures quickly and easily to communicate with all employees, Associates and visitors. This system is designed to help respond in a fast and decisive way during emergency situations. The multi-modal communications system, including phone, text, email, pagers, and more, allows NOAA to rapidly and efficiently reach our staff wherever they are. This ensures the life safety and security of all staff (including contractors) during emergencies.

The data collected contains personally identifiable information (PII) obtained from the NOAA Staff Directory (employees and contractors) and/or disclosed by the end-user for contacting in the case of emergency situations.

The encrypted PII/PHI collected for the medical library refers to federal employees (including NOAA Corps officers and U.S. Public Health Services (USPHS) officers). In some medical emergency instances, the reference may include contractors, members of the public, foreign nationals, and/or visitors. BII stored in AODocs libraries reference federal employees, contractors and commercial vendors.

Medical records on federal employees and contractors are imported into the AODocs library and protected using Google Drive's FIPS-140-2 compliant encryption at rest and Google Common Infrastructure. AODocs may contain Protected Health Information (PHI) or PII, such as full name, SSN, date of birth and email address.

Google Workspace collects email logs, authentication logs, basic user information, device information, calendar logs, vaccination information as a condition of employment, and drive logs. The PII and BII stored and transmitted by Google Workspace are at the discretion of the Data Owners.

Avaya One Cloud collects Name, Phone, Number, Email, Location, and Voicemail. The PII and BII stored and transmitted by Avaya One Cloud are at the discretion of the Data Owners.

Qualtrics collects survey information. The PII and BII stored and transmitted by Qualtrics are at the discretion of the Data Owners.

Entellitrak PII collected in the system consists of: employee's or applicant's name, functional limitation caused by the disability, reasonable accommodation (RA) requested, explanation of how RA would assist the applicant in the application process or the employee in performing his/her job or receiving the benefits and privileges of employment, dates when the required interactive discussions were held, notes from discussion regarding the request, action by deciding official, whether medical documentation was sought, justification for requesting medical documentation, any sources of technical assistance that were consulted, and if the request was denied, the reason for denial (but not medical documentation, which will be kept in a separate file).

MaaS360, Ivanti, Esri, and Smartsheet do not collect PII or BII.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There is the potential threat that the privacy data being processed by users could be intentionally or unintentionally disclosed or shared with other unauthorized users. However, this risk is moderate because of the access, physical, and logical security controls that are in place to prevent this from happening. NOAA requires the use of CAC cards for physical and network access, and roles and privileges for application authorization. In addition, NOAA users that are involved in the handling or processing of the privacy data for the hosted applications are required to review and sign the Rules of behavior and take mandatory training in order to minimize such risks. The users are required to adhere to NOAA's policies regarding disclosure and separation of duties.

AODocs is NOAA approved. AODocs claims security inheritance from other assessed products, and states "customer data stored in AODocs benefits from Google App Engine's security features, such as at rest encryption, the security of Google's network and the physical security of its datacenter facilities. Data storage in Google App Engine is highly redundant, with automatic replication across multiple datacenters." Additionally, Google Drive's FIPS-140-2 encryption has been implemented to provide additional protection for AODocs. AODocs relies on Google Workspace to comply with federal data privacy policies, laws and regulations

<u>Section 6</u>: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	X
DOC bureaus	X		
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			

Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: EBS connects with NOAA0700 which contains the NOAA staff directory. There is no direct connection. The data is loaded onto a server and is downloaded by EBS. ESRI connects with NOAA0700, NOAA ICAM service for authentication. However, no PII/BII is sent or received between the systems. G Suite applications ensure email communications and file collaboration within NOAA. AODocs shares data using the AODocs interface in G Suite, and data managed by AODocs is split between data hosted on the G Suite environment of the Customer (through the intermediary of technical "storage accounts") and in the backend of AODocs, hosted on Google Cloud Platform. ServiceNow does not share data within NOAA, users access data via a secure website https://nsdesk.service-now.com/
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.everbridge.com/no/about/legal/privacy-notice-2/ https://www.homelandsecurity.noaa.gov/ https://workspace.google.com/security/ https://www.servicenow.com/privacy-statement.html https://www.aodocs.com/terms-of-service https://privacy.microsoft.com/en-us/privacystatement https://cloudcheckr.com/cloudcheckr-data-security/ https://www.avaya.com/en/privacy/policy/ NOAA Certification for Vaccination PAS .	
X	Yes, notice is provided by other means.	Specify how: Photographic, Audio Recordings and Video recordings releases containing a Privacy Act Statement are obtained for all images of individuals.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For EBS, work related PII is automatically uploaded to the system from the staff directory; However, personal PII, e.g. personal cell phone number, is optional. For AODocs, individuals may decline during the collection of PII/BII. The individual can decline to provide audio, video or their image by not signing the release form. If an image has previously been uploaded to the web site, the individual can request to have the image removed from the web site.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For EBS, users are presented with the options on the staff directory screen where data is optionally entered. The only uses for the information in the staff directory are for contacting staff routinely, or once the information is in EBS, for contacting staff by EBS in emergencies.

		In accordance with the Privacy Act Statement, for AODocs, the medical library is configured to allow individuals to consent or decline uses of their PII/PHI. The proposed use of the photographic image, Audio Recordings and video recordings is described in the Likeness and Profile Release form. Individuals may decline to consent to a particular use of their image by not signing the image release form.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For EBS, users are presented with the option on the staff directory screen where data is optionally entered. This update reminder is displayed upon system entry for any purpose. For AODocs, based on document permissions, individuals may review and update PII/BII pertaining to them. Otherwise, individuals may contact the respective Library Administrator or AODocs System Administrator to update their PII/BII. An individual may request to have their audio, video or photographic image removed from an NOAA website at any time by contacting NOAA.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. **Explanation:** Access is tracked through established access control/audit.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 10/13/2021 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.

	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

All applications are encrypting based on FedRAMP requirements and adheres to the compliance standards of the Federal Information Processing Standard (FIPS). FedRAMP security controls encompass the accuracy, confidentiality, integrity, and availability of the information.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g,, name or Social Security number)?

_X__ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons **(AODocs)** COMMERCE/DEPT-2, Accounts Receivable **(MsDynamics)** COMMERCE/DEPT -7, Employee Accident Reports **(ServiceNow, AODocs, Everbridge)** COMMERCE/DEPT -18, Employees Personnel Files Not Covered by Notices of Other Agencies, **(Everbridge, AODocs)** COMMERCE/DEPT -25, Access Control and Identity Management System, **(Google Workspace)** COMMERCE/DEPT -31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations, **(G-Suite)** NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSO). **(AODocs)** OPM/GOVT-1, General Personnel Records, **(AODocs, ServiceNow)** OPM/GOVT-2,Employees Performance File Records **(AODocs)** OPM/GOVT-10, Employee Medical File System Records **(G-Suite)**
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Requirements for record retention are found in the NOAA Records Schedules : 100-24 Information Technology Operations and Management Records and 100-27 Records of the Chief Information Officer, p.12 and the GRS 3.1, 3.2, 4.1, 4.2, 5.8, and 6.3.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: The information collected allows for the identification of employees or contractors.

X	Quantity of PII	Provide explanation: PII is limited to contact information, Human Resources information, and some limited medical administrative information. As this information is collected across NOAA for multiple usage, the amount of information contained within this boundary is noted and will be larger than usual.
X	Data Field Sensitivity	Provide explanation: Sensitive PII, such as SSN, Taxpayer ID, Employer ID, financial and medical information is collected.
X	Context of Use	Provide explanation: Cloud applications residing in the NOAA0900 boundary are used for a variety of critical business processes that require the storing/transmission of PII/BII.
X	Obligation to Protect Confidentiality	Provide explanation: NOAA has the obligation to protect personal information collected in routine Human Resources operations. Additionally, some limited medical administrative data is collected (flight status). NOAA is obligated to protect this information. The Privacy Act of 1974 requires us to safeguard the collection, access, use, dissemination and storage of BII and PII.
X	Access to and Location of PII	Provide explanation: Access to each component application is managed through the respective application's access in that application's CSP. The location of the information resides within each CSP virtual environment.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

There is the potential threat that the privacy data being processed by users could be intentionally or unintentionally disclosed or shared with other unauthorized users. However, this risk is low because of the access, physical and logical security controls that are in place to prevent this from happening. NOAA requires the use of CAC cards for physical and network access, and roles and privileges for application authorization. In addition, NOAA users that are involved in the handling or processing of the privacy data for the hosted applications are required to review and sign the Rules of Behavior and take mandatory training annually (or as needed) in order to minimize such risks. The users are required to adhere to NOAA's policies regarding disclosure and separation of duties.

AODocs is NOAA approved. AODocs claims security inheritance from other assessed products, and states “customer data stored in AODocs benefits from Google App Engine’s security features, such as at rest encryption, the security of Google’s network and the physical security of its datacenter facilities. Data storage in Google App Engine is highly redundant, with automatic replication across multiple datacenters.” Additionally, Google Drive’s FIPS-140-2 encryption has been implemented to provide additional protection for AODocs. AODocs relies on Google Worksapce to comply with federal data privacy policies, laws and regulations.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.